ABSTRACT

A useful method of verifying the integrity of a cryptosystem involves using erroneous outputs to obtain secret information. In certain signature schemes which use the Chinese Remainder Theorem, a correct signature of a message and an erroneous signature of the same message permit the modulus to be easily obtained. If the content of the message is known, such cryptosystems may be cracked with only an erroneous signature of the message. Certain other authorization schemes may be cracked by analyzing a number of erroneous outputs caused by a particular type of error called a "register fault." A security expert or cryptosystem designer may intentionally induce a tamper proof device generate a faulty computation by subjecting the device, such as a smart card, to physical stress, such as certain types of radiation, atypical voltage levels, or a higher clock rate than the device was designed to accommodate. Cryptosystems should be impervious to the attacks described herein. If not, the system should be modified or discarded.